World Wide Web

Computer Emergency Response Team

Incident Report

Agency: **Date:**

Contact Name: **Phone:**

Email: **Fax:**

Virus/Intrusion Name:

Date of Incident: **Time of Incident:**

1. **Describe how the intrusion was discovered, its problems, systems affected, and damages:**
2. **Describe possible solutions for resolving the problems:**
3. **Describe recovery methods of system, information, data, networks, etc.:**
4. **Estimated date and time system will be available to users/customers:**
5. **Location of Computer System:**
6. **Is the affected system/network critical to the mission of the agency?** □Yes □No
7. **Is there evidence of spoofing?** □ Yes □ No □ Unknown
8. **Who is the anti-virus provider for the agency?**
9. **List the apparent source of the intrusion/attack (IP address), if known:**
10. **The last time the operating system was updated?**
11. **Please check type of problems and damages that apply:**

	□	Trojan Horse	□	Unauthorized Root Access	□	Network Damages
	□	Trapdoor	□	Web Site Defacement	□	Information/Data Damages
	□	Bomb	□	Denial of Service	□	Theft of Information/Data
	□	Worm	□	Distributed Denial of Service	□	Network Damages
	□	Hoax	□	Operating System Damages	□	Other, please describe:

12. **Suspected perpetrator or possible motivation of attack:**

	□	Insider/Disgruntled Employee	□	Former Employee	□	Domestic Perpetrator
	□	International perpetrator	□	Other, please describe:		

13. **What operating software systems were affected?**

	□	UNIX	□	Sun OS/Solaris	□	OS2
	□	LINUX	□	MacOS	□	Windows
	□	NT	□	Sun OS/Solaris	□	Other, Please describe:

14. What Hardware systems were affected?						
	□	Compaq	□	Packard Bell	□	Toshiba
	□	Dell	□	Apple	□	Micron
	□	HP	□	Gateway	□	PC Clone
	□	IBM	□	Fujitsu	□	Other, please describe:
15. CPU/Speed:						
	□	Pentium/90	□	Pentium/233	□	Pentium/400
	□	Pentium/100	□	Pentium/300	□	Pentium/450
	□	Pentium/133	□	Pentium/333	□	Motorola
	□	Pentium/200	□	Pentium/350	□	Other, please describe:
16. Memory:						
	□	16 MB	□	32 MB	□	64 MB
	□	128 MB	□	Other, please describe:		
17. Modem Speed:						
	□	28.8 baud	□	33.6 Baud	□	56 Baud
	□	ISDN	□	Other, please describe:		
18. Internet Browser:						
	□	Microsoft Internet Explorer	□	Netscape Navigator/Communicator	□	Other, please describe:
19. Agency Security Infrastructure (check all that apply):						
	□	CERT Team	□	Security Auditing Tool(s)	□	Secure Remote Access Tools
	□	Firewall(s)	□	Packet Filtering	□	Banners
	□	Intrusion Detection System(s)	□	Encryption	□	Account/Access Control List
	□	Other, please describe:				
20. What actions and technical mitigation have been taken?						
	□	System disconnected from network	□	System binaries checked	□	No action taken
	□	Backup of affected system(s)	□	Log files examined	□	Other, Please describe:
21. Critical State services affected (check all that apply):						
	□	Health	□	Transportation	□	Criminal Justice
	□	Public Safety	□	Agriculture	□	Education/Higher Ed.
	□	Corrections	□	Labor Employment	□	Revenue
	□	Environmental	□	Human/Social Services	☒	Administration
22. Please list other agency/organization that been informed? (Please provide names and phone numbers)						
	□	DPS	□	State SIPC		
	□	Attorney General	□	State CERT		
	□	Other, please describe:				